WEBBER WENTZEL

in alliance with > Linklaters

QUICK REFERENCE GUIDE:
CYBER SECURITY RISK MANAGEMENT

Data is perhaps the single most important asset for organisations with all organisations creating, collecting and using multitudes of different types of data. Given the value of data, it has become a target for those who seek to exploit it unlawfully resulting in a sharp rise in cyber-attacks, data theft and hacking.

This quick reference guide provides basic steps to manage and mitigate cyber security risks and sets out some basic "do's" and "don'ts".

PRE-BREACH: WHAT TO DO?

- **Ensure you have up-to-date IT and data security policies which comply with international best practice.**
  Use external technical service providers where necessary and ensure that your systems can identify any information affected so that you can act quickly and identify affected individuals. Also regularly monitor compliance with your IT and data security policy and test systems.

- **Review and assess key business contracts.**
  Revise employment contracts to ensure that employees are aware of their cyber security obligations. Employees travelling to high risk jurisdictions must take additional precautions. Also ensure that agreements with third party service providers comply with certain IT security industry standards and applicable laws. Note: contractual obligations may not be enough – you may need to undertake your own audits of providers.

- **Ensure that the board and staff understand the cyber security risks applicable to the business.**
  Identify gaps in awareness and understanding and provide training to supplement these gaps where needed. Training is not just a once off but a continuous process and is most effective when interactive and incorporates guidelines, handouts, visual aids and tailored roleplaying scenarios.

- **Take out a cyber insurance policy.**

- **Develop a data breach response plan.**
  Develop a response plan that is practical, up-to-date and easy to follow. Your response plan must identify a data breach lead and response team. The team should comprise of senior management, IT, public and investor relations, legal and compliance risk experts. Your response team should also include an external PR and legal. Remember, external legal teams are critical to ensure the benefit of legal privilege. Think carefully about how to activate the response team and ensure that the team lead has enough authority to investigate and make recommendations to the business. An effective plan includes strategies for managing different types of scenarios, a process for recording breaches and details of regulators and stakeholders that must be notified (and timelines for notification). The data breach response plan is focused on containing the breach, quickly assessing exposure and evaluating the risk and ensuring that people do not panic under pressure. It may be good to testing your response plans and training through controlled simulated data breach exercises.

- **Don't retain more information than you need**.
  Data is valuable, but risky – so keep only what you need.

POST-BREACH: WHAT TO DO

- **Manage civil and criminal actions** – either instituting against involved persons and / or defending claims against you.
- **Institute disciplinary action against negligent or wilful employees** (If appropriate).
- **Develop an action plan to determine areas of weakness and to ensure that further breaches are limited.**

WEBBER WENTZEL CYBER BREACH HOTLINE

+27 11 530 5554

cyberbreach@webberwentzel.com

KEY CONTACTS

Lisa Swaine
Insurance law and litigation
T: +27 11 530 5341
E: lisa.swaine@webberwentzel.com

Kim Rew
Insurance law and litigation
T: +27 21 431 7354
E: kim.rew@webberwentzel.com

Caroline Theodosiou
Insurance law and litigation
T: +27 11 530 5376
E: caroline.theodosiou@webberwentzel.com

Peter Grealy
Commercial law and regulatory
T: +27 11 530 5218
E: peter.grealy@webberwentzel.com

Nozipho Mngomezulu
Commercial law and regulatory
T: +27 11 530 5855
E: nozipho.mngomezulu@webberwentzel.com

Priyesh Daya
Litigation
T: +27 21 530 5358
E: priyesh.daya@webberwentzel.com

Dario Milo
Data breach litigation, communications and PR
T: +27 11 530 5232
E: dario.milo@webberwentzel.com

Berne Burger
Insurance law and litigation
T: +27 11 530 5878
E: berne.burger@webberwentzel.com

Justin Malherbe
Insurance law and litigation
T: +27 21 431 7364
E: justin.malherbe@webberwentzel.com

Karl Blom
Commercial law and regulatory
T: +27 11 530 5517
E: karl.blom@webberwentzel.com

Martin Hattingh
Litigation
T: +27 11 530 5976
E: martin.hattingh@webberwentzel.com

Ben Rule
Insurance law and litigation
T: +27 11 530 5447
E: ben.rule@webberwentzel.com

Cape Town
15th Floor, Convention Tower
Heerengracht, Foreshore,
Cape Town
8001
+27 21 431 7000

Johannesburg
90 Rivonia Road,
Sandton
Johannesburg
2196
+27 11 530 5000

About Webber Wentzel
We are the leading full-service law firm on the African continent, providing clients with seamless, tailored and commercially-minded business solutions within record times. Our alliance with Linklaters and our relationships with outstanding law firms across Africa ensures our clients have the best expertise wherever they do business.